Before The
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for	)	CC Docket No. 97-213
Law Enforcement Act	)	

COMMENTS OF SBC COMMUNICATIONS INC.

ROBERT M. LYNCH
ROGER K. TOPPINS
HOPE E. THURROTT

One Bell Plaza, Room 3023
Dallas, Texas 75202
214-464-3620

It's Attorneys

December 14, 1998

TABLE OF CONTENTS

SUMMARY

SBC strongly urges the Commission to adopt J-STD-025, without modification, as the appropriate technical standard for CALEA compliance. This standard already reflects compromises reached between the telecommunications industry and law enforcement. Moreover, it protects to the extent envisioned by Congress the privacy rights of individuals.

The purpose of CALEA was to permit law enforcement the same capabilities as it employed prior to CALEA's passage in relation to evolving technologies. In determining the proper parameters of the Act, Congress carefully balanced the concerns of law enforcement with individuals' rights to be protected from unwarranted invasions of privacy. This balance the industry has attempted to preserve is the interim industry standard.

The inclusion of any of the punch list items proposed by the DOJ/FBI in the technical standard adopted by the Commission would undercut Congressional intent and distort the clear meaning of the Act. In each instance, the requested item exceeds the parameters set by CALEA. Moreover, with regard to several of these features, the provision of the information is not "reasonably available" as required by the Act. The DOJ/FBI is seeking to circumvent Congress and have the Commission "interpret" the Act so as to allow it greater surveillance latitude than Congress had determined was justifiable. The inclusion of the punch list items in the technical standard by the Commission would enable law enforcement to achieve that which was considered and denied by Congress.

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for	)	CC Docket No. 97-213
Law Enforcement Act	)	

COMMENTS OF SBC COMMUNICATIONS INC.

SBC Communications Inc. files these comments, on its behalf and on behalf of its subsidiaries, (collectively referenced as "SBC") in response to the Further Notice of Proposed Rulemaking, released November 5, 1998 in the above captioned docket ("Further Notice") with respect to the technical standard to be adopted in fulfilling to the assistance capability requirements of the Communications Assistance for Law Enforcement Act ("CALEA" or "the Act"). Generally, the Further Notice seeks further comment related to the industry interim standard, J-STD-025, in light of matters raised in Petitions for Rulemaking filed by the Cellular Telecommunications Industry Association ("CTIA"), the Center for Democracy and Technology ("CDT"), the Department of Justice/Federal Bureau of Investigation ("DOJ/FBI") and the Telecommunications Industry Association ("TIA"), respectively. SBC continues to assert that the capabilities sought by the DOJ/FBI far exceed the parameters of CALEA and pose significant risks in relation to privacy rights. In addition, unless the DOJ/FBI affirmatively commits that it will reimburse the carriers for CALEA-related costs and follows through with this commitment, the cost burden related to compliance must, by necessity, be passed through to ratepayers to the extent allowed. To date, the DOJ/FBI, as evidenced by its cost

recovery rules, has sought to evade, rather than assume this obligation. These arguments and comments related to matters raised by the Commission are set forth below.

I. BACKGROUND

Section 103 of CALEA sets forth four "assistance capability requirements" which carriers must meet to comply with the CALEA dictates. Section 107(a)(2) allows that if a carrier, manufacturer or support service provider complies with publicly available technical requirements or standards adopted by the industry association or standard-setting organization, or by the Commission under Section 107(b), it has met the requirements of Section 103 and/or 106 as applicable.[1] A party can seek the Commission's involvement under Section 107 if the industry associations or standard-setting organizations failed to issue a technical standard or requirements or if a government agency or other person believed that the standard or the requirements issued fails to meet the four general assistance capability requirements of Section 103. Upon the filing of such a petition, the Commission is empowered to establish by rule the appropriate technical standard, taking into consideration the following five factors:

- Does the standard meet the assistance capability requirements of Section 103 by cost-effective means? ;
- Does the standard protect the privacy and security of communications not authorized by CALEA to be intercepted? ;
- Does the standard minimize the cost of CALEA compliance on residential ratepayers? ;
- Does the standard serve the policy of the United States to encourage the provision of new technologies and services to the public? and;

[1] While carriers are required to meet the requirements of Section 103, manufacturers and telecommunications support service providers are required by Section 106 to make available to carriers the features and modifications necessary for carriers to comply with the Section 103 requirements "on a reasonable timely basis and at a reasonable charge".

- Does the standard provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under Section 103 during any transition period?

Since 1995, the telecommunications industry has been attempting to reach a compromise with the DOJ/FBI which would result in a standard consistent with the language and intent of CALEA. Due to demands by the DOJ/FBI, which in the industry's opinion and the opinion of certain public interest groups, exceed the scope of CALEA, the industry was unable to develop a standard acceptable to law enforcement. Failing this attempt, the industry, by a unanimous vote through the Telecommunications Industry Association ("TIA"), adopted the industry interim standard, J-STD-025. It was, and remains the position of the industry, that this standard meets the requirements of CALEA and that compliance with this standard satisfies the "safe harbor" provision of Section 107.

Prior to the release of the interim industry standard, the Cellular Telecommunications Industry Association ("CTIA") filed a Petition for Rulemaking, arguing that the standard setting process was deadlocked. This petition attached a copy of what would eventually be designated as J-STD-025 and supported the adoption of this standard as fulfilling the dictates of CALEA. A second Petition for Rulemaking was filed by the Center for Democracy and Technology ("CDT") which argued that J-STD-025 went too far in permitting location information capabilities and failed to protect the privacy of packet-mode communications. CDT urged the adoption of a narrower standard, contending that J-STD-025 was not "reasonably available" under the Act. The third Petition for Rulemaking was filed by the DOJ/FBI which argued that the interim industry standard fails to provide all of the communications content and call-identifying information to which it believes it is entitled and further, fails to require the provisioning

of this information within the time periods requested by law enforcement. The DOJ/FBI set forth nine items (the "DOJ/FBI punch list") which it argued should be added to the interim standard. The fourth and final Petition for Rulemaking was filed by the TIA asking the Commission to resolve the dispute as to whether the interim standard is over-inclusive as argued by the CDT or under-inclusive as argued by the DOJ/FBI.

In response to the numerous petitions for extension filed by various parties, the date for compliance with the core features of CALEA was extended by the Commission to June 30, 2000. The basis for this extension was that compliance with the assistance capability requirements of Section 103 was not reasonably available by the prior October 25, 1998 date.

II. THE DEFINITION OF "REASONABLY AVAILABLE"

As the Commission has noted, in determining whether a specific technical requirement meets the dictates of Section 103, it must determine whether the information requested by law enforcement is "reasonably available". In doing so, SBC encourages the Commission to assess the following broad considerations: (1) the cost - e.g. is the cost for one feature disproportionately more than the cost attributable to the other CALEA features, jeopardizing the reimbursement to be received?; (2) the development period - e.g. can the technology be developed quickly enough such that it can be deployed within the legally prescribed period?; (3) the manufacturers' assessment of technical/technological feasibility and platform implementation - e.g. can the feature be deployed without requiring a wholesale redesign of the carrier's network? and; (4) logistics - e.g. is the call-identifying information available in the carrier's switch?

In applying these factors in the context of CALEA, call-identifying information is reasonably available if the information is present at an Intercept Access Point ("IAP") for

call processing purposes and major modification to the switch to support this functionality is not necessary. The IAP for this discussion's purpose is the central office switch. Network protocols should not need to be modified solely for purposes of providing call-identifying information. In addition, wholesale modifications to upstream billing and service order operations support systems should not be mandated in order to attain other information, such as customer name and address, that is not reasonably available in the IAP switch. The specific elements of call-identifying information which are reasonably available at the IAP are likely to vary dependent upon the different technologies and will change as technologies change.

III. COST ANALYSIS

The Commission further requests detailed cost data related to the adding of a feature to the carrier's network.[2] SBC has provided wireline carrier cost estimates which will be included with other carriers' figures in the Comments to be filed by the United States Telephone Association ("USTA") in this proceeding. The industry has worked closely with manufacturers in an attempt to evaluate nationwide aggregate costs. Prior conversion estimates were provided to Congress by Roy Neel, President and CEO of USTA, in his testimony of October 23, 1997.[3] Mr. Neel testified that the interim industry standard alone would cost approximately $1.2 billion dollars to implement. It is believed by SBC that the inclusion of the DOJ/FBI punch list items in the standard would double these costs. The $500 million established in CALEA for this purpose obviously will be grossly inadequate.

---

[2] Further Notice, ¶30.

[3] Testimony of Roy Neel, President and CEO of USTA, before the Crime Subcommittee of the House Judiciary Committee, October 23, 1997.

However, the Commission must bear in mind that the cost information provided is preliminary only. There exists far too many unknown variables to submit accurate information. One of these unknown variables relates to whether the DOJ/FBI will fund manufacturers' software costs for CALEA directly or whether the carriers will be invoiced associated Right-To-Use ("RTU") fees. If required to pay these fees, carriers could spend hundreds of thousands of dollars per switch on RTU fees alone. Given that the number of switches impacted within SBC is likely to exceed 850, this variable significantly effects the final cost figure.

Another significant unknown variable relates to the uncertainty concerning an appropriate Call Content Channel/Call Data Channel provisioning model related to the number of channels SBC will be required to deploy per switch. Despite repeated requests for clarification by SBC and the industry, DOJ/FBI has still failed to provide the information that would enable SBC to deploy the appropriate amount of capacity at each switch. In addition, the proposed separated delivery also results in confusion related to the projection of CALEA costs and the correct provisioning of CALEA capacity. This factor alone could potentially double anticipated CALEA-related costs.

If dialed digit extraction is provided, costly tone receivers that would be dedicated full-time for each surveillance must be added to our switches. This dramatically affects our call content channel capacity costs. Without knowing the capacity requirements per surveillance SBC cannot project CALEA costs accurately.

In determining the impact of CALEA related costs on residential ratepayers, the answer lies with the willingness of law enforcement to bear the costs related to its demands. As the cost recovery rules adopted by the DOJ/FBI illustrate, the DOJ/FBI is unwilling to assume this obligation, even given the clear intent of CALEA that it do so.

If law enforcement does not pay these CALEA-related costs, carriers may have little choice but to pass these costs on to their ratepayers, if permitted to do so by law.

IV. TIMELINE FOR IMPLEMENTATION OF TECHNICAL REQUIREMENTS

SBC is unable to comply with the Commission's request that it supply a projected timeline for each technical requirement, setting forth the time needed to develop, test and deploy it. To estimate the development and test time for each requirement would require input from manufacturers that SBC has not requested. Although SBC has directed its vendors to develop products which will conform with J-STD-025, it has not made any requests with regard to the disputed features proposed by the DOJ/FBI. Thus, there is no information currently available upon which to base an accurate timeline.

V. THE INTERIM INDUSTRY STANDARD, J-STD-025

A. CAPABILITIES OF J-STD-025 OPPOSED BY THE CDT

The Commission has determined to limit its review of the interim standard whether the location information and packet-mode provisions currently included in the standard and the nine punch list items sought by the DOJ/FBI which have not been included meet the assistance capability requirements of Section 103. SBC believes that the CDT's opposition to the provisioning of location information is based upon a misunderstanding of the standard's requirements. J-STD-025 would have a carrier identify the location of a subject's "mobile terminal" whenever the information is reasonably available at the IAP and its delivery to law enforcement is legally authorized. While a majority of the switch platforms are capable of determining the identification of the cell sites for both the origination and termination of the call, some switch platforms in use today cannot provide the identification of the cell site for the termination of the call

when the call is handed over to a different Mobile Telephone Switching Office ("MTSO"). SBC believes that the location information encompassed by the interim industry standard is call-identifying information under CALEA.

The interim standard also allows for law enforcement to access call-identifying information and to intercept wire and electronic telecommunications, regardless if the transmission is in circuit-mode or packet-mode. The CDT objects to the allowance of packet-mode interception. Specifically, CDT is concerned that carriers are not required to separate call content information from packets before their delivery to law enforcement, when only call-identifying information is authorized for delivery.

The simple answer to this concern is that carriers cannot feasibly separate such information such that carriers can provide separate packet headers only on call-identifying information. This is because packet-mode communications, unlike more traditional telecommunications services, operate by combining the call-identifying information and the content in a single protocol data "packet", which are not separable given the current competitive and service quality imperatives that the marketplace is applying to data communications. Data traffic is growing at exponential rates, and all of the industry's innovation is aimed at accelerating the processing and routing of data packets in order to meet customers' demand for faster transmission times. Thus, wherever possible, the routing of packets is being embedded in hardware or firmware, and "self-routing" techniques are being developed to bypass the current structure of using software algorithms to examine each packet. These technical innovations, which eliminate the software processing of data packets, will also eliminate the ability to separate call-identifying information from data content without slowing down transmission speeds so much that the service would be of little value to customers. Every

data packet would have to be slowed down and broken apart, not only those subject to surveillance orders, because there is no way to identify a packet by subscriber until it is "read".

Other differences between packet communications and traditional telecommunications also weigh heavily against any requirement that call-identifying information be separated from packet content. Data networks, unlike their "POTS" counterparts, have a large number of different interfaces, protocols, interconnection architectures, etc. Many of these features are evolving rapidly, on a day-to-day basis, as providers search for better, faster ways to serve their customers. Each of these different structures would require its own set of standards to permit separation of packet content form call-identifying information. Network configuration is another concern: there no longer is any central point, such as the switch serving the surveillance target number, where all of the call-identifying information is "known" and can be retrieved. Instead, details such as calling and called number, time of call and time of disconnection are established and recorded, if at all, only by non-network components such as users' personal computers and privately-owned network servers. Coupled with the vastly increased costs that packet separation would require, which costs would be embedded in the prices of switches, routers and other network equipment, these facts amply demonstrate that separating packet content from call-identifying information would not be reasonably available. SBC agrees with the Commission's observation that the imposition of any technical requirements on packet-mode communications is premature. The compromise represented by J-STD-25 in this regard should not be disturbed.

B. THE DOJ/FBI PUNCH LIST

1. General Comments

The interim industry standard was not developed in a vacuum, with disregard to law enforcement's demands. Where feasible, the proposals of law enforcement were incorporated into the standard. The interim standard already reflects a compromise on the part of the industry, albeit not to law enforcement's total satisfaction. However, it continues to be the position of SBC that two requirements have yet to be met by the DOJ/FBI to support its demands for additional features beyond that which the interim industry standard currently offers: (1) legal support for the contention that these features are within the purview of CALEA and; (2) fair reimbursement for costs incurred to implement these additional capabilities. Although the DOJ/FBI claims that its punch list is "firmly rooted in the language, legislative history and policies of CALEA", SBC and the industry have yet to see any evidence to this effect. No legal analysis to support this broad claim has been presented. Instead, the DOJ/FBI would have the Commission and the industry rely upon its unsubstantiated assurances.

Moreover, contrary to the assertions of the DOJ/FBI, the goal of CALEA's assistance capability requirements is to ensure that the technical ability of law enforcement to carry out electronic surveillance meets, rather than exceeds, law enforcement's current surveillance capabilities. CALEA is intended to maintain law enforcement's abilities to conduct surveillance in a rapidly evolving telecommunications technology, not to grant law enforcement the authority to employ further invasive measures in disregard of the provisions of the law and of individuals' privacy rights. In its Committee Reports on CALEA, Congress made the following statement concerning

the intended interpretation of the law:

> "The Committee intends the assistance requirements in section 2602 [now 47 U.S.C. §10002] to be both a floor and a ceiling. The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past. The Committee urges against overbroad interpretation of the requirements. The legislation gives industry, in consultation with law enforcement and subject to review by the FCC, a key role in developing the technical requirements and standards that will allow implementation of the requirements. The Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements."[4]

Each of the enhanced surveillance capabilities on the punch list represents a sharp departure from these principles of CALEA interpretation.

2. Conference Calls Without "Target Party" on Line.

The DOJ/FBI would have the Commission believe that Title III[5] permits a court-ordered intercept of any communications "supported by" a target subject's equipment, facilities or services, regardless of whether or not the target party, i.e. the party named in the court order, is actually on the line. Accordingly, the DOJ/FBI maintains that Section 103 of CALEA requires carriers to provide the capability to monitor the conversations of parties to a three-way or conference call with a *target after the target has dropped off the line or place the other parties on hold.* Yet, the DOJ/FBI has admitted that failure to provide this capability "...does not amount to a reduction in the information that has been available to law enforcement..." prior to CALEA.[6] J-STD-25 maintains the status quo, and as such meets that which is required under CALEA.

---

[4] House Report 103-827, at pp. 22-23.

[5] 18 U.S.C. §2510, *et seq*.

[6] Joint Petition for Expedited Rulemaking filed by the DOJ/FBI on March 27, 1998, ¶51, page 30.

Additionally, it should be noted that this capability would exceed the clear language of Section 103(a)(1) of the Act, which requires that law enforcement be able to intercept only communications *to or from* equipment, facilities or services of a subscriber. The interim standard also properly provides for delivery to law enforcement of all communications that can be heard by persons using the target facilities.

Moreover, SBC agrees with AirTouch that this feature can be easily bypassed by individuals seeking to evade surveillance and, as such, would be an ineffective, as well as costly, feature. SBC further concurs with the position taken by TIA that this item would expand beyond existing precedent the scope of Title III. Until now, the term "facilities" in this context has pertained only to the subscriber's terminal equipment. There is no viable justification beyond the wishes of the DOJ/FBI to ignore this interpretation.

Nor in all instances is the interception of a conference call reasonably available. Only if the conferencing occurs within the parameters of an individual carrier's CALEA-equipped switch is the interception of a call in which the subscriber has dropped off reasonably available. However, interception of any other conference call outside this scope is not likely to be reasonably available. While a carrier in these circumstances may provide the information requested for a subscriber, it cannot always technically cover parties outside the scope of the subscriber's switch.

3. Party hold, join, drop on conference calls.

This punch list item would permit law enforcement to require from a carrier messages identifying the parties to a conference call conversation at any time. The party-hold message would be provided when any party is placed on hold. The party-join message would report the addition of a party to an existing call or the reactivation of a held call. The party-drop message would report when a party to the call is released or

disconnected and the call continues. SBC disputes the DOJ/FBI contention that this item is necessary under CALEA. These messages will not indicate a party's participation in a call. In addition, the information is not call-identifying information; "call-identifying information" means the signals, pulses or tones that initially set up and direct a call, not signals, etc. sent after a call is established. Nor is this information under all circumstances reasonably available to the carrier. For example, a call placed on hold by a party utilizing his customer premises equipment is not detectable at the carrier's switch. Moreover, if the conference bridge is not within a single carrier's switch, the messages are incapable of being sent.

It is unreasonable to place carriers in the position of having to monitor the attendance of all parties to a call. Requiring carriers to provide on-going information related to call participation clearly exceeds the carriers' obligations under CALEA.

4. Subject-initiated dialing and signaling information

This item of law enforcement's wish list involves the use of feature keys, flash hook presses, and dialing of digit keys for various purposes following initial establishment of the call ("cut-through"). Once again, these signals do not fit the traditional concept of "call-identifying information". Furthermore, to the extent that they have not previously been available through pen register intercepts, they constitute access to additional information that Congress expressly stated it did not intend to provide in CALEA. Thus, CALEA's legislative history clarifies that Congress did not intend to require that these messages be added to the long-standing industry definition of "call-identifying information".

SBC further opposes the inclusion of this feature in the industry standard on the basis that it is not always reasonably available. Only if the subscriber action can be

"read" within a CALEA-equipped switch, does the feature meet this standard. At this time, it is unknown whether a signal of this nature can be incorporated into the switch by manufacturers at a reasonable cost.

5. In-band and out-of-band signaling

In its arguments on this item, the DOJ/FBI again exceeds CALEA's definition of "call-identifying information". Network-generated signals such as call waiting, ringing or busy signals have nothing to do with origin, direction, destination or termination of a call. In addition, these tones cannot be detected from the network or the originating or terminating switches; thus, they are not reasonably available to carriers. In any event, to the extent that these signals can be audibly detected over the target subscriber's line, they constitute *call content*, and can be obtained through a properly authorized Title III intercept. Certain types of in-band and out-of-band signaling constitute call content information, including ISDN user-to-user signaling and ISDN D-channel packet data transmission. If they cannot be audibly detected, they are neither call content nor call-identifying information, and therefore are, not covered by CALEA.

6. Timing information

SBC continues to assert that timing of the delivery of call-identifying information is a function of network and equipment design. The time "delay" is a matter of seconds. Whether the information is available in 3 seconds or 30 seconds will make no difference with regard to law enforcement's objective. To cite a kidnapping as an example of law enforcement's need for this feature is ludicrous; a delay of seconds will have no impact on law enforcement's ability to prevent or end the commission of such a crime. Despite these scare tactics, the DOJ/FBI can point to no actual case in which the timing of a carrier's delivery of call-identifying information has ever led to a crime that otherwise

would have been prevented. More importantly, the fact is that timing of delivery of call-identifying information is a function of network and equipment design, and thus law enforcement is prohibited from dictating an arbitrary timing requirement by Section 103.

What is far more critical is the synchronization of timestamps within a switch which would enable the accurate association of call content to call-identifying information, rather than the actual delivery time. In discussions between the industry and law enforcement, law enforcement has sought to impose unrealistic and unreasonable timing requirements in the order of 100 milliseconds. Yet if this unnecessary standard were achievable, a conclusion by no means certain, it would require the extensive and costly redesigning of a carrier's timing and synchronization network.

Imposing strict demands of this nature could also lead to a loss of content. Some manufacturers' designs using dial up CCC content channels result in a loss of content entirely for the first few seconds of the transmission after which the delivery is concurrent with the call. Despite this glaring deficiency, the DOJ/FBI was amenable to this delivery because it is less costly. Yet, even under these circumstances, call completion time for dialed-up CCCs are subject to the same statistical variations that apply to any call completed within the public switched network. It is not possible due to the characteristics of the network to assure law enforcement that this information can be provided within 3 seconds, much less 100 milliseconds.

In addition, even if carriers were to attempt to employ this feature, timestamps for content are not going to necessarily be synchronized across a network or with relation to multiple network elements in the carrier's network or outside networks. The discrepancy involved could easily exceed 3 seconds, and will most certainly exceed 100 milliseconds. Additional complexities might be posed depending upon how law enforcement envisions

the sequence of events which would occur with regard to two separate surveillances in different parts of the country. To implement an accurate, nationwide synchronization of all switches in order to provide these timestamps is clearly not reasonably available since it would require a drastic, wholesale redesign of all carriers' networks. Achieving 100 milliseconds delivery as law enforcement requests may require the extensive and costly redesign of a carrier's timing and synchronization network.

7. Surveillance status

These features have nothing to do with call-identifying information or the content of communications. They merely verify that an intercept is operational, a function that is adequately provided for in the interim standard. While CALEA requires that carriers ensure their capability of intercepting communications and isolating call-identifying information, CALEA does not require that carriers constantly confirm this to law enforcement in real time. Test procedures already are available by which law enforcement can perform this function in concert with carrier personnel. Again, the DOJ/FBI petition here seeks to dictate the manner in which the industry complies with CALEA, which Congress expressly intended to leave to carriers.

8. Continuity check tone

The continuity check tone capability requested would require a carrier to place a C-tone or dial tone on the call content channel (CCC) received by law enforcement until a user of the facilities under surveillance initiates or receives a call, at which point the tone would be turned off. CALEA does not require continuity tone capability. However, while the DOJ/FBI has proposed a relatively complex surveillance status message with regard to surveillance status, it may be possible that a simple continuity check tone on call content channels could be employed to notify law enforcement when a surveillance is

active. This method would avoid the need for human intervention to periodically check the circuit manually. While SBC continues to assert that this capability is not required by CALEA, the continuity check tone is a possible compromise approach which may be more cost effective to implement than the surveillance status message.

9. Feature status

This technical capability would require a carrier to notify law enforcement when specific subscription based calling services are added to or deleted from facilities under surveillance. SBC agrees with the Commission that this capability is not required by CALEA as call-identifying information. In order to provide this information in an automated fashion at the time the subscriber submits a request would require the reconfiguration of the carriers' customer services databases and other related software. It is not "reasonably available" to mandate measures which would require the wholesale redesign of the network simply to comply with law enforcement's preferences regarding surveillance. While it is necessary for changes in the telephone number of the facilities to be conveyed to law enforcement, this need is already being met through existing administrative procedures.

10. Dialed digit extraction

This technical capability would require a carrier to provide law enforcement any digits dialed by the subject after connecting to another carrier's service ("post-cut-through digits"). Not all of the information involved is call-identifying information readily available to the carrier. Credit card numbers and automated queuing system responses are unrelated to call routing and completion. Moreover, the delivery of this information would not protect the privacy of certain content communications, the interception of which has not been lawfully authorized. A carrier simply has no means of segregating

protected communications. The technology does not distinguish between post-cut-through digits that are call-completion oriented and those which constitute call-content.

If law enforcement has Title III authorization, it has no need for dialed digit extraction since it thereby has a CCC channel which enables it to receive all dialed digit information. Thus, the implementation of this significantly expensive feature is unwarranted.

With respect to these functions, law enforcement once again argues with the industry over the manner in which delivery of call-identifying information will take place. The DOJ/FBI argues that CALEA requires carriers to "employ the most efficient and effective means of delivering authorized surveillance information to law enforcement". SBC is unable to find any such requirement specified in CALEA; rather, it is clear from the legislative history that Congress intended for the determination of the methods of CALEA compliance to be left to the industry.

VI. DISPOSITION OF J-STD-025

As discussed above, it remains SBC's position that J-STD-025 should be adopted, without modification, as the final industry standard. However, should deficiencies be found, the Commission should refer the standard back to Subcommittee TR45.2 of TIA for revision. Whether such activity can be completed within 180 days will, of course, depend upon the extent of the Commission's modifications.

However, the Commission is unduly optimistic when it concludes that the industry can unquestionable comply with the June 30, 2000 deadline in relation to the implementation of J-STD-025 core requirements. Preliminary data from two of SBC's primary suppliers indicates that their initial CALEA partially-compliant products will not be available until second quarter 2000. This provisioning will not allow for the extensive

testing required to ensure the deployment is in compliance with the industry standard, nor does it allow a sufficient period for the deployment across SBC's entire network. Due to the number of switches which will be effected, SBC is concerned that nationwide implementation by the June 30th date is infeasible.

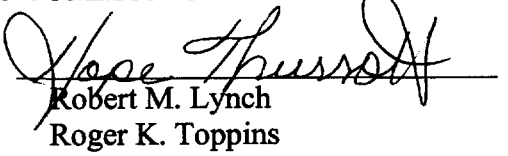
There is also some confusion as to what standard the carriers will be held on the June 30, 2000 date. In paragraph 32 of the Further Notice, the Commission states that in order to satisfy the safe harbor requirements of Section 107(a), carriers must comply with whatever industry standard the Commission ultimately adopts in this proceeding. Yet, in paragraph 133 of the Further Notice, the Commission states that carriers will be expected to comply with the core requirements of J-STD-025 by the June 30, 2000 date. Will compliance with the J-STD-025 core requirements by the June 30th deadline allow carriers to avail themselves of the "safe harbor" provision? If not, then the deadline should be extended until compliance with the revised standard is achievable.

VII. CONCLUSION

CALEA represents a compromise; the privacy rights of individuals balanced against the desires of law enforcement to maintain surveillance capabilities in light of evolving technology. The nine punch list item proposed by the DOJ/FBI for inclusion in the technical assistance capabilities standard exceed the scope of CALEA's requirements and, in effect, circumvent the careful balancing Congress intended to achieve with the Act. For this reason, SBC strongly encourages the Commission to adopt J-STD-025 as the appropriate industry standard without modification.

Respectfully submitted,

SBC COMMUNICATIONS INC.

By: 

Robert M. Lynch
Roger K. Toppins
Hope Thurrott
One Bell Plaza, Room 3023
Dallas, Texas 75202
214-464-3620

Attorneys for
SBC Communications Inc. and its
Subsidiaries

December 14, 1998

Certificate of Service

I, Mary Ann Morris, hereby certify that the foregoing "Comments of SBC Communications, Inc.," in CC Docket No. 97-213 has been served on December 14, 1998 to the Parties of Record.

Mary Ann Morris

December 14, 1998

PAMELA J RILEY
DAVID A GROSS
AIRTOUCH COMMUNICATIONS INC
1818 N STREET NW
SUITE 320 SOUTH
WASHINGTON DC 20036

BARBARA J KERN
AMERITECH CORPORATION
2000 WEST AMERITECH CENTER DRIVE
ROOM 4H74
HOFFMAN ESTATES IL 60196

STEVEN SHAPIRO ESQ
AMERICAN CIVIL LIBERTIES UNION
125 BROAD STREET
18TH FLOOR
NEW YORK NY 10004

JOHN T SCOTT III
CROWELL & MORING LLP
ATTORNEYS FOR BELL ATLANTIC MOBIL
INC
1001 PENNSYLVANIA AVENUE NW
WASHINGTON DC 20004

DAVID L SOBEL ESQ
ELECTRONIC PRIVACY INFORMATION CTR
666 PENNSYLVANIA AVE SE
SUITE 301
WASHINGTON DC 20003

M. ROBERT SUTHERLAND
THEODORE R KINGSLEY
BELLSOUTH CORP
SUITE 1700
1155 PEACHTREE STREET N E
ATLANTA GEORGIA

BARRY STEINHARDT ESQ
ELECTRONIC FRONTIER FOUNDATION
1550 BRYANT ST
SUITE 725
SAN FRANCISCO CA 94103-4832

ALAN R SHARK
AMERICAN MOBILE
TELECOMMUNICATIONS ASSOCIATION IN
1150 18TH ST NW SUITE 250
WASHINGTON DC 20036

ELIZABETH R SACHS ESQ
LUKAS MCGOWAN NACE & GUTIERREZ
1111 19TH STREET NW
SUITE 1200
WASHINGTON DC 20036

MICHAEL P GOGGIN
BELLSOUTH CELLULAR CORP
SUITE 910
1100 PEACHTREE STREET NE
ATLANTA GA 30309-4599

J LLOYD NAULT II
BELLSOUTH TELECOMMUNICATIONS INC
4300 BELLSOUTH CENTER
675 WEST PEACHTREE STREET NE
ATLANTA GA 30375

MICHAEL ALTSCHUL
RANDALL S COLEMAN
CELLULAR TELECOMMUNICATIONS
INDUSTRY ASSOCIATION
1250 CONNECTICUT AVENUE NW
SUITE 200
WASHINGTON DC 20036

DANIEL J WEITZNER
JAMES X DEMPSEY
CENTER FOR DEMOCRACY AND
TECHNOLOGY
1634 EYE STREET NW
SUITE 1100
WASHINGTON DC 20006

STANTON MCCANDLIS
ELECTRONIC FRONTIER FOUNDATION
1550 BRYANT STREET SUITE 725
SAN FRANCISCO CA 94103-4832

JOHN F RAPOSA
RICHARD MCKENNA
GTE SERVICE CORPORATION
600 HIDDEN RIDGE HQE03J36
PO BOX 152092
IRVING TX 75015-2092

GAIL L POLIVY
GTE SERVICE CORPORATION
1850 M STREET NW
SUITE 1200
WASHINGTON DC 20036

JAMES TO ROCHE
TIMOTHY S SHEA
GLOVECAST NORTH AMERICA INC
400 NORTH CAPITOL STREET NW
SUITE 880
WASHINGTON DC 20001

HENRY M RIVERA
LARRY S SOLOMON
J THOMAS NOLAN
M TAMBER CHRISTIAN
ATTORNEYS FOR METRICOM INC
GINSBURG FELDMAN & BRESS CHTD
1250 CONNECTICUT AVENUE NW
WASHINGTON DC 20036

RICHARD C BARTH
MARY E BROONER
MOTOROLA INC
SUITE 400
1350 I STREET NW
WASHINGTON DC 20005

ANDY ORAM
COMPUTER PROFESSIONALS
FOR SOCIAL RESPONSIBILITY
PO BOX 717
PALO ALTO CA 94302

CAROLYN G MORRIS
U S DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
J EDGAR HOOVER BUILDING
935 PENNSYLVANIA AVENUE NW
WASHINGTON DC 20535

H MICHAEL WARREN
CALEA IMPLEMENTATION SECTION
FEDERAL BUREAU OF INVESTIGATION
14800 CONFERENCE CENTER DRIVE
SUITE 300
CHANTILLY VA 20151

STEWART A BAKER
THOMAS M BARBA
MAURY D SHENK
STEPTOE & JOHNSON LLP
1330 CONNECTICUT AVENUE NW
WASHINGTON DC 20036

DAVID COSSON
L MARIE GUILLORY
NATIONAL TELEPHONE
COOPERATIVE ASSOCIATION
2626 PENNSYLVANIA AVENUE NW
WASHINGTON DC 20037

ROBERT S FOOSANER
LAWRENCE R KREVOR
LAURA L HOLLOWAY
NEXTEL COMMUNICATIONS INC
1450 G STREET NW
SUITE 425
WASHINGTON DC 20005

EMILIO W CIVIDANES
RONALD L PLESSER
PIPER & MARBURY LLP
ATTORNEYS FOR OMNIPOINT
COMMUNICATIONS INC
1200 19TH STREET NW
WASHINGTON DC 20036

LISA M ZAINA
STUART POLIKOFF
OPASTCO
21 DUPONT CIRCLE NW
SUITE 700
WASHINGTON DC 20036

JUDITH ST LEDGER-ROTY
PAUL G MADISON
KELLEY DRYE & WARREN LLP
ATTORNEYS FOR PAGING NETWORK INC
1200 19TH STREET NW SUITE 500
WASHINGTON DC 20036

ERIC W DESILVA
STEPHEN J ROSEN
WILEY REIN & FIELDING
ATTORNEYS FOR PERSONAL
COMMUNICATIONS INDUSTRY ASSOC
1776 K STREET NW
WASHINGTON DC 20006

MARK J GOLDEN
MARY E MADIGAN
PERSONAL COMMUNICATIONS INDUSTRY
ASSOCIATION
500 MONTGOMERY STREET SUITE 700
ALEXANDRIA VA 22314-1561

MICHAEL K KURTIS
JEANNE W STOCKMAN
KURTIS & ASSOCIATES PC
ATTORNEYS FOR POWERTEL INC
2000 M STREET NW
SUITE 600
WASHINGTON DC 20036

WILLIAM L ROUGHTON JR
PRIMECO PERSONAL
COMMUNICATIONS LP
601 13TH STREET NW
SUITE 320 SOUTH
WASHINGTON DC 20005

CARESSA D BENNET
DOROTHY E CUKIER
BENNET & BENNET PLLC
ATTORNEYS FOR RURAL
TELECOMMUNICATIONS GROUP
1019 19TH STREET NW
SUITE 500
WASHINGTON DC 20036

CAROLE C HARRIS
CHRISTINE M GILL
ANNE L FRUEHAUF
MCDERMOTT WILL & EMERY
ATTORNEYS FOR SOUTHERN
COMMUNICATIONS SERVICES INC
600 THIRTEENTH STREET NW
WASHINGTON DC 20005

JOSEPH R ASSENZO
SPRINT SPECTRUM LP d/b/a SPRINT PCS
4900 MAIN STREET 12TH FL
KANSAS CITY MO 64112

MATTHEW J FLANIGAN
GRANT SEIFFERT
TELECOMMUNICATIONS INDUSTRY ASSN
1201 PENNSYLVANIA AVENUE NW
SUITE 315
WASHINGTON DC 20004

STEWART A BAKER
THOMAS M BARBA
BRENT H WEINGART
L BENJAMIN EDERINGTON
STEPTOE & JOHNSON LLP
COUNSEL FOR TIA
1330 CONNECTICUT AVENUE NW
WASHINGTON DC 20036

KEVIN C GALLAGHER
360° COMMUNICATIONS COMPANY
8725 W HIGGINS ROAD
CHICAGO IL 60631

PETER M CONNOLLY
KOTEEN & NAFTALIN
ATTORNEYS FOR UNITED STATES
CELLULAR CORPORATION
1150 CONNECTICUT AVENUE NW
WASHINGTON DC 20036

LAWRENCE E SARJEANT
LINDA KENT
KEITH TOWNSEND
UNITED STATES TELEPHONE ASSOCIATIO
1401 H STREET NW SUITE 600
WASHINGTON DC 20005

KATHRYN MARIE KRAUSE
EDWARD M CHAVEZ
DAN L POOLE
U S WEST INC
1020 19TH STREET NW SUITE 700
WASHINGTON DC 20036

WILLIAM T LAKE
JOHN H HARWOOD II
SAMIR JAIN
TODD ZUBLER
WILMER CUTLER & PICKERING
2445 M STREET NW
WASHINGTON DC 20037-1420

KURT A WIMMER ESQ
GERARD J WALRON ESQ
ALANE C WEIXEL ESQ
COVINGTON & BURLING
1201 PENNSYLVANIA AVENUE NW
P.O. BOX 7566
WASHINGTON DC 20044-7566

MICHAEL W WHITE
BELLSOUTH WIRELESS DATE LP
10 WOODBRIDGE CENTER DRIVE
4TH FLOOR
WOODBRIDGE NJ 07095-1106

CHARLES M NALBONE
BELLSOUTH PERSONAL
COMMUNCIATIONS INC
SUITE 400
3353 PEACHTREE ROAD NE
ATLANTA GA 30326

JOYCE & JACOBS
ATTORNEYS AT LAW LLP
1019 19TH STREET NW
14TH FLOOR PH #2
WASHINGTON DC 20036

LOUIS J FREEH
LARRY R PARKINSON
FEDERAL BUREAU OF INVESTIGATION
935 PENNSYLVANIA AVENUE NW
WASHINGTON DC 20535

THE HONORABLE JANET RENO
ATTORNEY GENERAL OF THE
UNITED STATES
U S DEPARTMENT OF JUSTICE
601 D STREET NW
ROOM 9106
WASHINGTON DC 20530

STEPHEN W PRESTON
DEPUTY ASSISTANT ATTORNEY GENERAL
U S DEPARTMENT OF JUSTICE
601 D STREET NW
ROOM 9106
WASHINGTON DC 20530

DOUGLAS N LETTER
APPELLATE LITIGATION COUNSEL
U S DEPARTMENT OF JUSTICE
601 D STREET NW
ROOM 9106
WASHINGTON DC 20530

SCOTT R MCINTOSH
DANIEL KAPLAN
ATTORNEYS APPELLATE STAFF
CIVIL DIVISION
U S DEPARTMENT OF JUSTICE
601 D STREET NW
ROOM 9106
WASHINGTON DC 20530

MARTIN L STERN
LISA A LEVENTHAL
PRESTON GATES ELLIS & ROUBELAS
MEEDS LLP
1735 NEW YORK AVENUE NW
SUITE 500 WASHINGTON DC 20006

MICHAEL W MOWERY
AIRTOUCH COMMUNICATIONS INC
2999 OAK ROAD MS1025
WALNUT CREEK CA 95596

WILLIAM F ADLER
GLOBALSTAR LP
3200 ZANKER ROAD
SAN JOSE CA 95134

WILLIAM D WALLACE
CROWELL & MORING LLP
1001 PENNSYLVANIA AVENUE NW
WASHINGTON DC 20004

MARK C ROSENBLUM
AVA B KLEINMAN
SETH S GROSS
AT&T CORP
ROOM 3252F3
295 NORTH MAPLE AVENUE
BASKING RIDGE NJ 07920

REX L FULLER III
5900 SHIRL COURT
CHESAPEAKE BEACH MD 20732

DOUGLAS I BRANDON
AT&T WIRELESS SERVICES INC
FOURTH FLOOR
1150 CONNECTICUT AVE
WASHINGTON DC 20036

CATHERINE WANG
MICHAEL P DONAHUE
SWIDLER BERLIN SHEREFF
FRIEDMAN LLP
3000 K STREET NW
SUITE 300
WASHINGTON DC 20007

MATTHEW J WHITEHEAD II
AMERICAN MOBILE SATELLITE
CORPORATION
300 KNIGHTSBRIDGE PARKWAY
LINCOLNSHIRE IL 60069

JOHNNIE L SMITH
DIVISION OF NARCOTICS ENFORCEMENT
123 W WASHINGTON AVE
7TH FLOOR
P O BOX 7857
MADISON WI 53707-7857

JEROME S CAPLAN
REDCOM LABORATORIES INC
ONE REDCOM CENTER
VICTOR NY 14564

JAMES F IRELAND
THERESA A ZETERBERG
COLE RAYWID & BRAVERMAN LLP
1919 PENNSYLVANIA AVENUE NW
SUITE 200
WASHINGTON DC 20006

JOY ROBERTSON
REGULATORY & GOVERNMENT AFFAIRS
8350 EAST CRESCENT PARKWAY
SUITE 400
ENGLEWOOD CO 80111

ALBERT GIDARI
PERKINS COIE LLP
1201 THIRD AVE 40TH FLOOR
SEATTLE WA 98101

MAGALIE ROMAN SALAS
OFFICE OF THE SERETARY
FEDERAL COMMUNICATIONS
COMMISSION
THE PORTALS 445 TWELFTH STREET SW
ROOM TW-A325
WASHINGTON DC 20554
(ORIGINAL AND 4 COPIES)

INTERNATIONAL TRANSCRIPTION
SERVICE
1231 20TH STREET NW
WASHINGTON DC 20036